SKOPENOW

THE DEFINITIVE GUIDE

OSINT Workflows for Tackling Disinformation

Skopenow.com

Introduction

The Importance of Verification in OSINT

Information is abundant and easily accessible via the internet. However, the sheer volume of data presents a significant challenge: how do we separate fact from fiction?

For OSINT practitioners, the ability to verify and authenticate information is critical.

The intelligence we produce directly influences decision-making processes, potentially impacting lives and organizations.

Understanding Unreliable Information in OSINT

Disinformation

Definition: False information deliberately created and spread to deceive.

Characteristics:

- Often has a specific agenda or motive (political, economic, or social)
- Professionally crafted to appear credible
- Strategically disseminated through multiple channels

Example: State-sponsored campaigns spreading false narratives about geopolitical events.

Misinformation

Definition: Inaccurate information spread without malicious intent.

Characteristics:

- Often results from misunderstanding or lack of fact-checking
- Can spread rapidly, especially on social media
- May originate from credible sources making honest mistakes

Example: Outdated statistics being shared as current facts.

Subject Deception Attempts

Definition: Efforts by investigation subjects to mislead investigators.

Characteristics:

- Can range from simple omissions to elaborate false narratives

- Often involves manipulating digital footprints
- May include creating fake online personas or altering existing profiles

Example: A subject creating a social media post to establish an alibi.

Outdated or Historical Information

Definition: Once accurate information that has become obsolete over time.

Characteristics:

- Often found in older records or databases
- May appear credible due to its official or commercial source
- Particularly common with personal contact information or addresses

Example: A five-year-old consumer database listing an individual's previous address and phone number.

AI Hallucinations

Definition: Plausible but fabricated information generated by AI models.

Characteristics:

- Often appears coherent and context-appropriate
- May blend real and fictitious details seamlessly
- Can be challenging to distinguish from accurate information
- More likely to occur when AI is asked about specific or obscure topics

Example: An AI-generated report describing a non-existent meeting between two world leaders, complete with fabricated quotes and outcomes.

Key Takeaways

1. Each type of unreliable information presents unique challenges for verification.
2. The lines between these categories can often blur, complicating the verification process.
3. Understanding these distinctions is crucial for developing effective verification strategies.

As OSINT professionals, our job is to navigate this complex landscape. We must remain vigilant and skeptical, always questioning the authenticity and reliability of the information we encounter.

Foundational Principles of Verification in OSINT

Source Evaluation

Always start by scrutinizing the source of information.

Key questions to ask:

- Who is behind this information?
- Do they know the information first-hand?
- What is their expertise or authority on the subject?
- Do they have a history of reliability or any known biases?

Techniques:

- Check author credentials and background
- Evaluate the reputation of the author or publishing platform
- Look for transparency in sourcing and methodology

Source Evaluation

Commercial vs. public sources:

- **Commercial sources:** Often more structured but may have access restrictions
- **Public sources:** More diverse but can be less regulated

Reliability considerations:

- Commercial sources aren't inherently more reliable; they may have different biases or data collection methods, such as bias towards individuals with larger digital footprints
- Public sources may offer more recent or real-time information in some cases

Cross-Referencing and Corroboration

Never rely on a single source of information.

Process:

- Seek out multiple independent sources
- Compare details across different accounts
- Look for consensus among reputable sources

Remember: Quantity doesn't equal quality. Five unreliable sources don't outweigh one highly credible source.

Contextual Analysis

Information doesn't exist in a vacuum; context is crucial.

Aspects to consider:

- **Historical context:** How does this fit with established facts?
- **Cultural context:** Are there cultural nuances affecting interpretation?
- **Temporal context:** When was this information created or last updated?
- **Motivational context:** What might be the reasons for sharing this information?

This principle helps identify anomalies and inconsistencies that may not be apparent at first glance.

Critical Thinking and Bias Awareness

Our own biases can significantly impact verification efforts.

Key practices:

- Regularly challenge your own assumptions
- Be open to information that contradicts your expectations
- Actively seek out diverse perspectives

Techniques:

- Play devil's advocate with your findings
- Engage in peer review when possible
- Use structured analytical techniques to mitigate cognitive biases

Key Takeaways

1. These principles should be applied throughout the verification process, not just at the beginning or end.
2. They work in concert - no single principle is sufficient on its own.
3. Developing these as habits will significantly enhance the quality and reliability of your OSINT work.

By internalizing these foundational principles, you'll be better equipped to tackle the practical workflows we'll discuss next.

Impact of Disinformation

Key Risks and Harmful Effects

- **Political Manipulation** – Used to sway public opinion, influence elections, and destabilize governments.
- **Financial Manipulation** – Can distort markets, drive stock fluctuations, and enable fraud.
- **Health Misinformation** – Undermines public health efforts, spreads harmful treatments, and erodes trust in medical institutions.
- **Threats to Investigations** – Misleads investigators, obscures truth, and diverts resources from legitimate cases.
- **Security Risks** – Facilitates cyber threats, reputational harm, and erosion of trust in institutions.

Practical Workflows for Verification

Initial Triage of Information

Quick credibility checks

1. Use the SIFT method:
    a. Stop - Pause before sharing or acting on information
    b. Investigate the source
    c. Find alternative coverage
    d. Trace claims to the original context
    e. Check the URL: Look for unusual domains or slight misspellings of reputable sites
    f. Scan for red flags: Excessive ads, poor grammar, sensationalist language

Red flags and warning signs

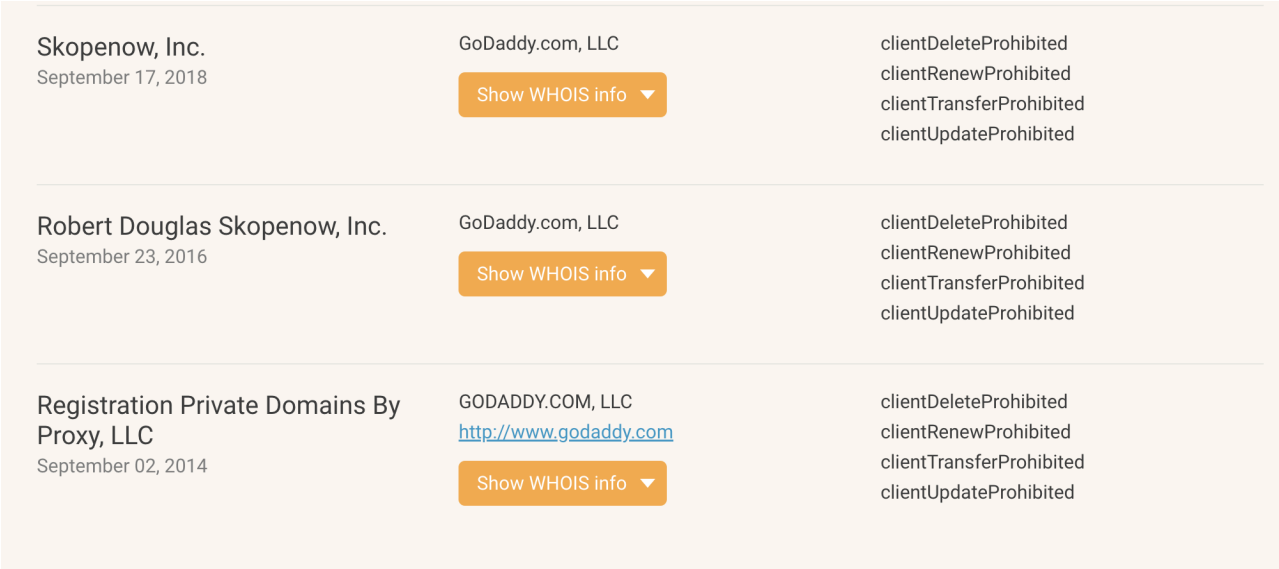
1. Lack of dates or bylines
2. No cited sources or references
3. Claims of exclusive information or "what they don't want you to know"
4. Emotional manipulation or urgency to share

In-depth Verification Process

Source tracking and evaluation

1. Use tools like Whois lookup for website ownership
    a. https://whois.easycounter.com/domain.com to include historical data
2. Check author profiles across multiple platforms

3. Evaluate the source's track record and reputation in the field with the 3x5x2 system



In the standardized 3x5x2 system, intelligence grading is expressed via numerical and alphabetical values.

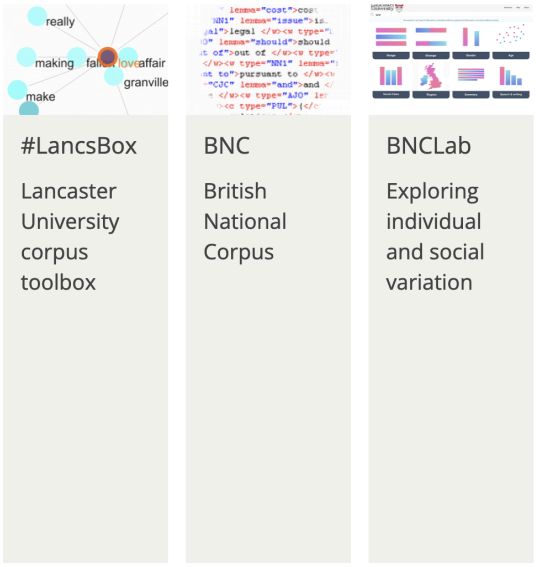
Source Evaluation (Reliability)	Information Evaluation (Validity)	Handling Conditions
1 - Reliable	A - Known directly to the source	P - Lawful sharing permitted
2 - Untested	B - Known indirectly to the source but corroborated	
	C - Known indirectly to the source	C - Lawful sharing permitted with conditions
3 - Unreliable	D - Not known	
	E - Suspected to be false	

Based on the reliability and validity grading of intelligence, an investigator or analyst can very quickly determine its strength, ensuring the reliability of evidence.

	3 - Unreliable	2 - Untested	1 - Reliable
B - Known indirectly to the source but corroborated	Medium	High	High
A - Known directly to the source	Low	Medium	High
C - Known indirectly to the source	Low	Low	Medium
D - Not known	Low	Low	Low
E - Suspected to be false	Low	Low	Low

Content analysis techniques

1. **Fact-checking:** Cross-reference key claims with authoritative sources
2. **Linguistic analysis:** Look for inconsistencies in tone, style, or terminology
    a. https://www.clarin.ac.uk/resources
    b. Phrase frequency analysis
    c. Specific sentence construction
    d. Reliance on certain grammatical tics like using a lot of adverbs
3. **Reverse image search:** Use tools like TinEye or Google Image Search
4. **Prejudice:** Identify potential bias or agenda
5. **Accuracy:** Check for sensationalism or emotional manipulation

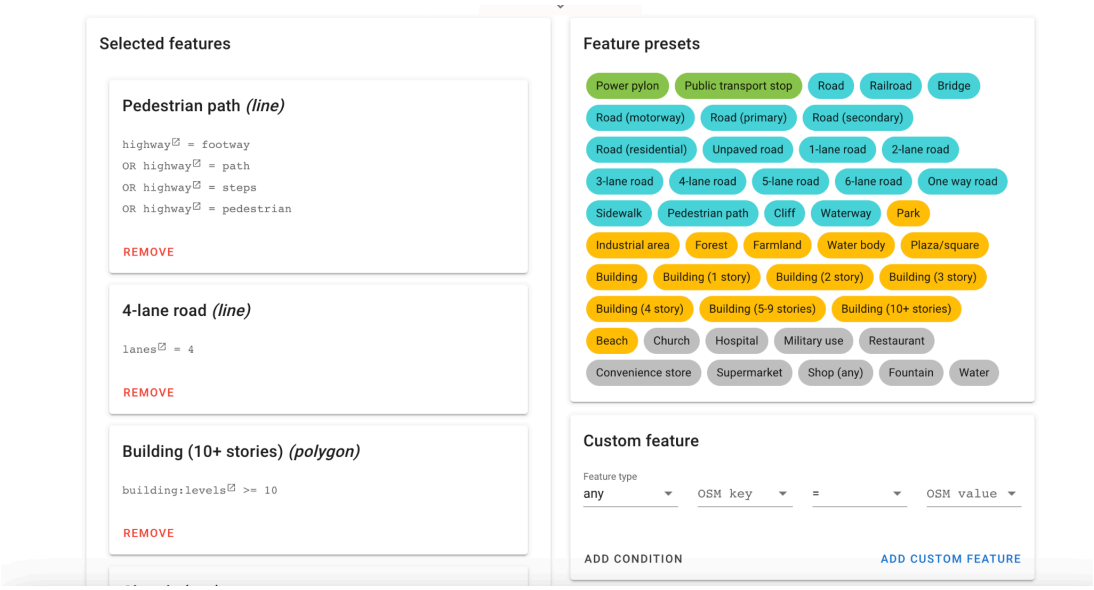


Temporal and geospatial verification

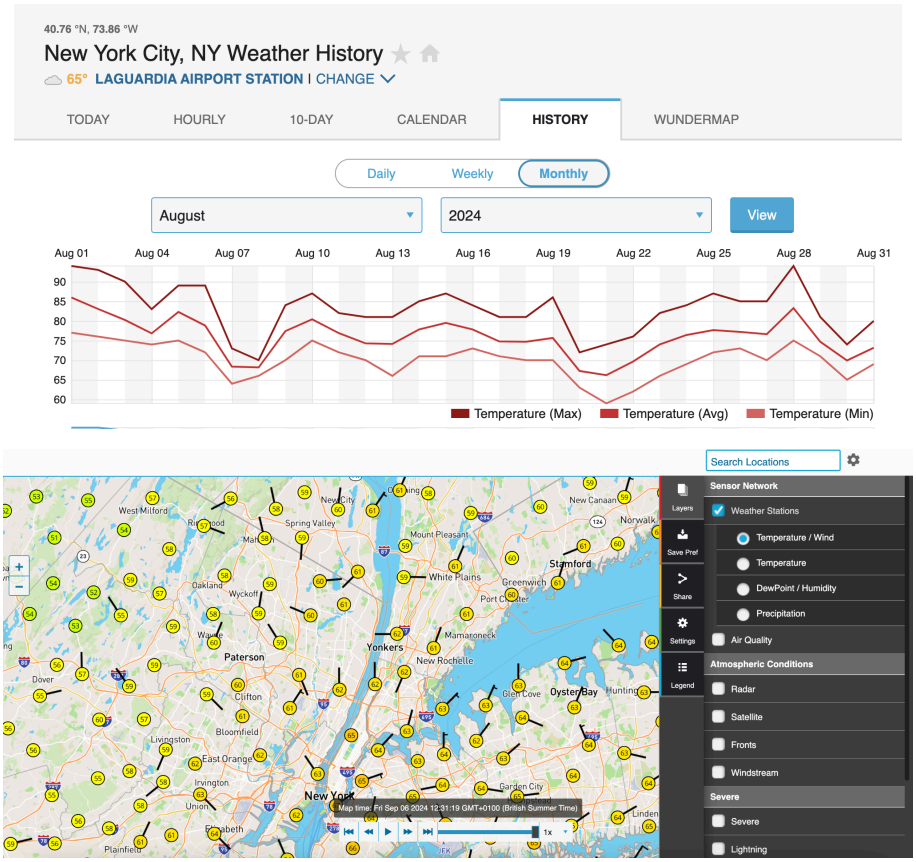
- **Timeline analysis:** Create a chronology of events to spot inconsistencies
  - https://timeline.knightlab.com/
- **Introduce anchor points:** Cross-reference with known facts and events

Temporal and geospatial verification

- **Geolocation:** Use tools like Google Earth, Bellingcat's Openstreetmap search tool https://osm-search.bellingcat.com/, or GeoSpy https://geospy.web.app/



- **Weather verification:** Cross-reference claimed conditions with historical weather data
    - https://www.wunderground.com/history/daily/KLGA/date/2024-9-6

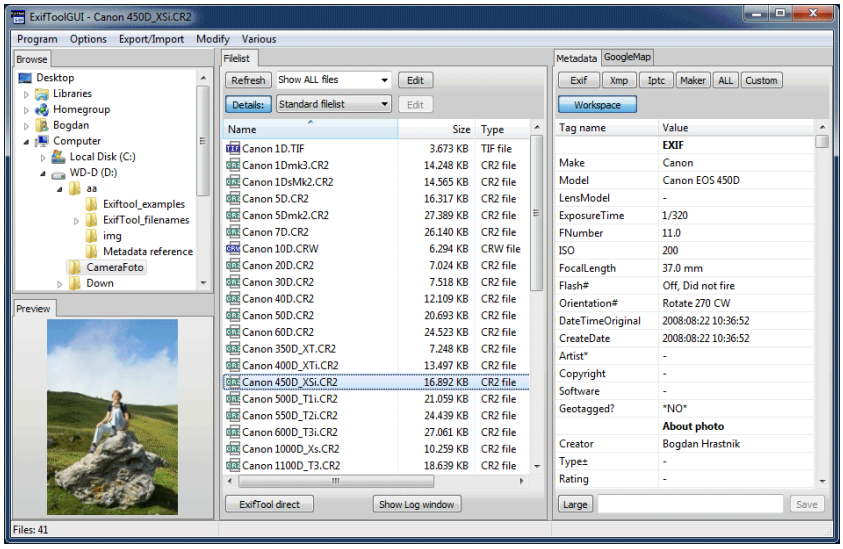


Timeliness verification

1. Check the date of data collection/ creation or last update
2. For personal information, look for recent activity or corroboration
3. Use multiple sources to create a timeline of information accuracy
4. Evaluate relevance to current context
5. Be cautious of using single-point-in-time data for current assessments

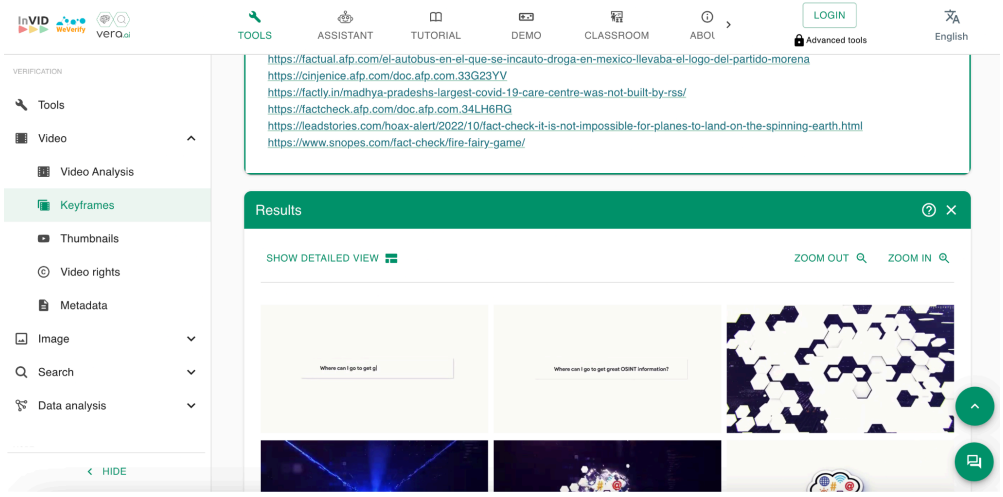
Digital Forensics Techniques for OSINT - Metadata analysis

1. Use an exif/ metadata viewer for image and document metadata
    a. https://exiftool.org/
2. Look for discrepancies between metadata and claimed origin/timeline



Digital Forensics Techniques for OSINT - Image and video verification tools

1. **Forensically:** Analyse image manipulation
    a. https://29a.ch/photo-forensics/#forensic-magnifier
2. **InVID:** For video analysis, verification, and keyframe analysis
    a. https://www.invid-project.eu/
3. **FotoForensics:** Detect image editing and manipulation
    a. https://fotoforensics.com/



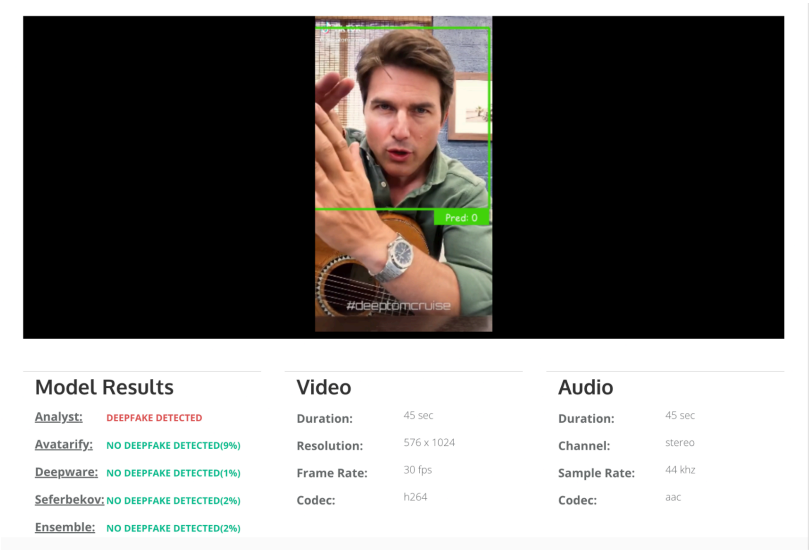
Disinformation/Misinformation Assessment

1. Identify potential motives for spreading false information
2. Check for known disinformation narratives or techniques
3. Assess virality and spread patterns to determine patterns of amplification, i.e. Hoaxy

4. Evaluate emotional appeal and polarizing elements

Digital Forensics Techniques for website and social media authentication

1. **Analyze images and video for deepfake indicators:**
    a. https://scanner.deepware.ai/
    b. https://weverify.eu/tools/deepfake-detector/
2. **Archive.org's Wayback Machine: Check website history**
    a. https://web.archive.org/
3. **Botometer: Detect potential bot accounts**
    a. https://botometer.osome.iu.edu/



Corroboration Strategies

1. Triangulate information from multiple diverse sources, including commercial and free sources
2. Prioritize primary sources over secondary or tertiary ones, at least with free sources
3. Be aware of circular reporting (multiple outlets citing a single original source)
4. Cross-reference information between commercial and public sources
    a. Be aware of potential circular reporting between these source types
    b. Use public sources to verify the currentness of commercial data
5. Consider expert consultation:
    a. Leverage specialist communities (e.g. Subreddits)
    b. Use platforms like Discord and Slack to speak with other OSINT specialists for collaborative verification
    c. Consult subject matter experts when dealing with specialized topics

Contextual Analysis

- **Historical context**

    - How does the information fit into the broader historical narrative?
    - Are there any historical precedents or patterns relevant to this information?
    - How might past events influence the current situation?
- **Cultural context**
    - Are there cultural nuances or sensitivities that could affect interpretation?
    - How might cultural differences impact the creation or dissemination of this information?
    - Are there any cultural biases (yours or the source's) to be aware of?
- **Motivational context**
    - What might be the reasons for sharing or creating this information?
    - Are there potential personal, political, or economic motivations at play?
    - How might these motivations affect the reliability of the information?
- **Broader informational ecosystem context**
    - How does this information fit into the larger narrative or discourse?
    - Are there competing narratives or counter-narratives to consider?
    - How is this information being shared and discussed in different communities or platforms?

Critical Thinking and Bias Check

1. **Team discussion to challenge assumptions**
    a. Consider diverse perspectives and apply a devil's advocate
2. **Apply structured analytical techniques**
    a. Analysis of Competing Hypotheses (ACH) – develop a set of different hypotheses
    b. Key Assumptions Check - question the investigator's assumptions
    c. Quality of Information Check - score by source type
3. **Consider alternative hypotheses**
    a. Brainstorm multiple explanations and assess the probability of each hypothesis
    b. Look for information that might disprove your leading theories
4. **Reflect on personal and organizational biases**
    a. **Confirmation Bias:** Seeking information that confirms existing beliefs
    b. **Anchoring Bias:** Over-relying on the first piece of information encountered
    c. **Availability Bias:** Overestimating the likelihood of events with greater "availability" in memory
    d. **Groupthink:** Prioritising harmony or conformity in the group over critical evaluation

Authenticity Scoring

1. Assign weighted scores to each verification step (1-10)
2. Calculate an overall authenticity score
3. Classify information:

a. **Confirmed** (90-100%)
b. **Highly Probable** (75-89%)
c. **Probable** (60-74%)
d. **Possible** (40-59%)
e. **Unlikely** (20-39%)
f. **Highly Unlikely** (1-19%)
g. **Disproven** (0%)

Confidence Assessment

- Evaluate the following factors:
    - Quantity and quality of sources
    - Consistency across multiple verification methods
    - Strength of corroborating evidence
    - Expertise level of the investigation team in the subject matter
    - Completeness of available information
    - Time constraints on the investigation
    - Historical accuracy of similar information/sources

- Assign a confidence level:
    - **High Confidence (85-100%)**: Strong evidence from multiple high-quality sources, consistent across verification methods, few or no information gaps
    - **Moderate Confidence (70-84%)**: Good evidence, mostly consistent, some minor gaps or uncertainties
    - **Low Confidence (50-69%):** Some evidence, but significant inconsistencies or gaps in information
    - **Very Low Confidence (below 50%):** Weak or conflicting evidence, major information gaps

- Combine authenticity score and confidence level:
    - Example: "Highly Probable (80%) with Moderate Confidence (75%)"

Systematic Approach to Credibility Assessment

Documentation

1. **Maintain detailed records**
    a. Log all steps taken in the verification process
    b. Note the tools used and their results
2. **Create an audit trail**

    a. Save screenshots or archives of original sources
    b. Document any changes or updates to the information over time
3. **Be transparent about limitations**
    a. Clearly state any uncertainties or gaps in verification
    b. Explain the reasoning behind credibility assessments

Documentation Steps

1. Compile detailed verification process notes
2. Archive original sources and verification evidence
3. Clearly state any limitations or uncertainties
4. Prepare final report including:
    a. Authenticity assessment and reasoning
    b. Confidence level and justification
    c. Combined authenticity and confidence statement
5. Provide any necessary caveats or contextual information for interpreting the scores

Peer Review and Validation

1. Internal team review of findings and process
    a. A pair of fresh eyes can assess:
    b. Methodology adherence
    c. Logic of conclusions
    d. Quality and reliability of sources
    e. Potential biases or blind spots
2. Address any discrepancies or concerns raised
3. Additional data collection or analysis
4. Re-evaluation of sources or methodologies
5. Consensus-building discussions
6. Clearly document differing viewpoints if consensus can't be reached

Workflow Integration

- Start with initial triage to quickly filter out obviously unreliable information
- For information that passes initial triage, apply in-depth verification processes
- Use digital forensics techniques to dig deeper into questionable content
- Always corroborate findings with multiple sources and expert input when necessary

Remember, these workflows are not linear - you may need to cycle back to earlier steps as new information emerges. The key is to remain flexible and thorough in your approach.

Developing a Standardized Workflow

1. **Create a checklist**
    a. Incorporate all key verification steps
    b. Include source evaluation, content analysis, and corroboration
2. **Establish clear criteria for credibility levels**
    a. e.g., Confirmed, Highly Probably, Probable, Possible, Unlikely, Highly Unlikely, & Disproven
3. **Implement a confidence scoring system**
    a. Assign weights to different verification factors using a numerical scale (e.g., 1-10) for each criterion
    b. Assign an overall confidence score, e.g. High Confidence, Moderate Confidence, Low Confidence, and Very Low Confidence
4. **Set thresholds for action**
    a. Define minimum credibility scores for different uses of information
5. **Implement source-specific verification protocols**
    a. Develop separate checklists for commercial and public sources
    b. Include steps to verify the timeliness and currentness of information
    c. Establish procedures for handling potentially outdated personal information

Continuous Learning and Adaptation

1. **Stay updated on new verification tools and techniques**
    a. Follow OSINT communities and thought leaders
    b. Regularly attend training and workshops
2. **Conduct post-mortems/ autopsies on significant cases**
    a. Analyze what worked well and what could be improved
    b. Update your workflow based on lessons learned
3. **Adapt to evolving threats**
    a. Stay informed about new forms of disinformation or deception
    b. Adjust your verification processes accordingly

Key Takeaways

1. A systematic approach ensures consistency and reduces the risk of oversight.
2. Documentation is crucial for both accountability and continuous improvement.
3. The field of OSINT verification is dynamic - your approach should evolve with it.

By implementing this systematic approach, you'll not only improve the reliability of your OSINT work but also build trust with decision-makers who rely on your intelligence.

The goal is not just to verify individual pieces of information, but to develop a robust, repeatable

process that can withstand scrutiny.

Challenging Disinformation in Analysis Across Your Organization

6 Strategies for Navigating Bias with Diplomacy

1. **Always Verify Sources** – Encourage tracing claims back to the original source before accepting them. Use a simple verification checklist.
2. **Use Non-Confrontational Corrections** – Ask questions like, "Where did this originate?" instead of outright dismissing information.
3. **Recognize Bias** – Frame bias as a universal challenge. Red-team exercises can help analysts challenge their own assumptions.
4. **Treat Social Media as Low-Reliability** – Implement a "Trust Ladder," where social media claims require higher verification before being used.
5. **Allow Face-Saving Corrections** – If someone falls for disinformation, let them revise their stance without embarrassment.
6. **Depoliticize the Process** – Frame verification as professional tradecraft, not ideological bias. Use neutral examples to build credibility.

Automating Investigations with Skopenow

Skopenow is one of the most comprehensive open-source intelligence platforms on the market. The company has over 1,500 customers, including 20% of the Fortune 500 as well as numerous large government and law enforcement agencies. Leveraging advanced AI, Skopenow quickly analyzes and interprets millions of publicly accessible data points, providing valuable insights through an integrated product suite. Founded in 2016 and headquartered in New York City, Skopenow is a venture-backed technology company with a distributed team across the globe. For more information, visit www.skopenow.com.